

SCANNED

UNITED STATES DISTRICT COURT

for the
District of MaineU.S. DISTRICT COURT
PORTLAND, MAINE
RECEIVED AND FILED
U.S. DISTRICT COURT
PORTLAND, MAINE
2012 MAY 18 PM 4:33In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The residence at 198 Concord Street, Portland, Maine;
See ATTACHMENT ACase No. 11-MAJ-1110-JHR

DEPUTY CLERK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the _____ District of _____ Maine _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

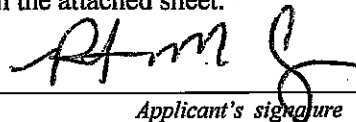
The search is related to a violation of:

Code Section
18 U.S.C. §§ 2252, 2252AOffense Description
Relating to the knowing transportation, shipment, receipt, possession, distribution, and reproduction of child pornography

The application is based on these facts:

See Affidavit of Special Agent Patrick M. Clancy

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Patrick M. Clancy, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/06/2011

A TRUE COPY
ATTEST: Christa K. Berry, Clerk
Judge's signature

City and state: Portland, Maine

John H. Rich III, U.S. Magistrate Judge

Printed name and title

By: 
Deputy Clerk

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR
A WARRANT TO SEARCH AND SEIZE**

Filed pursuant to Local Rule 157.6(a)

I, Patrick M. Clancy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 198 Concord Street, Portland, Maine, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. This application seeks authority for a warrant to search for and seize evidence, fruits, and instrumentalities of violations of, among other statutes, Title 18, United States Code, Section 2252 and Title 18, United States Code, Section 2252A, which relate to the knowing transportation, shipment, receipt, possession, distribution, and reproduction of child pornography.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been employed as a Special Agent since 2004 and I am currently assigned to the Boston Division, Portland Resident Agency. During my tenure with the FBI, I have participated in numerous criminal investigations, to include matters involving child pornography. In my career as an FBI Special Agent, I have utilized various investigative tools and techniques to include the use of search warrants. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my

participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

TECHNICAL TERMS

3. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Peer-to-peer file-sharing" ("P2P") is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running

compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

PROBABLE CAUSE AND BACKGROUND OF INVESTIGATION

4. I have received and read copies of reports prepared by FBI Task Force Officer (TFO) Nicholas Rudman III describing his investigation. The information contained in the paragraphs below is derived from those reports and from my conversations with TFO Rudman. TFO Rudman has been a sworn law enforcement officer since 1997, and an investigator since 2003. TFO Rudman has been investigating internet crimes, including investigations related to child pornography, since 2008. Since October of 2010, TFO Rudman has been a member of an FBI cyber crimes task force located in Virginia.

5. As part of an undercover investigation, TFO Rudman assumed an online username on a publically available P2P file-sharing network. This network is similar to a social networking site in which users can accept "friend" requests from other users and also send "friend" requests to other users. On April 12, 2011, TFO Rudman received a friend request from username "someone9423" to the undercover username used by TFO Rudman. TFO Rudman accepted the friend request from "someone 9423."

6. On April 13, 2011, TFO Rudman signed on to the P2P network using the previously mentioned undercover username. TFO Rudman observed that "someone9423" was logged on. TFO Rudman connected to the user "someone9423" and previewed thumbnail images of child erotica and child pornography in the shared folders of user "someone9423."

7. At approximately 11:01 a.m. on April 13, 2011, TFO Rudman, using his undercover on-line identity, selected and downloaded two(2) video and two (2) picture files from the shared folder "TW." At approximately 11:57 a.m. on April 13, 2011, TFO Rudman, using his undercover on-line identity, selected and downloaded one (1) video from the shared folder "TW." The folder "TW" was 19.39 gigabytes and most if not all the files in the folder had child pornography terms in the file names, such as "jacks bro off. . .," "Dad cums in boy," and "I Best from boy porn"

8. TFO Rudman recorded these undercover sessions in real time and I have viewed these recordings and the referenced downloads.

9. I have reviewed the five (5) files that TFO Rudman downloaded from the shared directory of "someone9423." Based on my experience and training, I have concluded that the files depict minors engaged in sexually explicit conduct. The files are described briefly below:

- a. A JPEG image file named "7 2 Adorable Gay Preteen Boys So Cute Get Their Fun On 8yo S" downloaded from a shared directory of "someone9423." The image depicts a prepubescent male whose mouth is around another prepubescent male's penis.
- b. A JPEG image file named "Little 8Yo Preteen Boy Sucks 9Yo Friend As They Both Jack Daddy - Kdv Rizmasta Rizmasta Pjk Rbv Pthc Pedo Kiddy R@Ygold Cp Boys Preteens (1)" downloaded from a shared directory of "someone9423." The image depicts a shirtless prepubescent male whose mouth is around a nude prepubescent male's penis. In the image, both prepubescent males are touching another male's penis.
- c. A Windows Media Audio/Video file named "I new ! (pthc) 2007 tara 8yr - the sensual side" downloaded from a shared directory of "someone9423." During the six minute and ten second video, a prepubescent female with brown hair, nude except for a purple and gold mask, lies on a bed while fondling her nipples and

vagina. I know from training and experience that "pthc" stands for "pre-teen hard core."

- d. A FLV file named "! O aa 5yo JASON 7yo JOSH – moreno" downloaded from a shared directory of "someone9423." During the two minute and twenty-five second video, two nude prepubescent males are sitting on a bed fondling their penises. Later in the video, the pre-pubescent males perform fellatio on one another.
- e. A Video Clip file named "Karin 10yo P" downloaded from a shared directory of "someone9423." During the five minute and twenty eight second video, a nude minor female with brown hair sits on a couch and inserts a blue object in her vagina. The video also contains close up video of the minor female inserting a blue object in her vagina.

Printed copies of the JPEG image files described in subparagraph (a) and (b) are attached under seal and labeled EXHIBIT 1A and EXHIBIT 1B, respectively. A copy of the three video clips described in subparagraphs (b), (c), and (d) are attached under seal on a computer disk labeled Exhibit 2.

10. TFO Rudman used the software program CommView to identify the internet protocol (IP) address used by "someone 9423," during the April 13, 2011, undercover sessions, as 76.178.243.56. A query of the American Registry of Internet Numbers (ARIN) IP database revealed that the IP address 76.178.243.56 resolved to Time Warner Cable Communications. TFO Rudman caused an administrative subpoena to be served on Time Warner Cable Communications for records relating to IP address 76.178.243.56 for the dates and times that TFO Rudman had downloaded the four files from the shared directory of "someone9423." The response from Time Warner Cable Communications to that subpoena shows that at the dates and times of that downloads the IP address was assigned to the account registered to Linda Fenton,

198 Concord Street, Portland, Maine, user name LFENTON@maine.rr.com and FentonJ87@maine.rr.com, telephone number 207-774-0656.

11. Publicly available telephone directory information shows 207-774-0656 as the residential listing telephone number for John and Linda Fenton, 198 Concord, Portland, Maine.

12. A review of the City of Portland Assessor's office Online Database revealed the owners of 198 Concord Street, Portland, Maine, to be John P. and Linda A. Fenton. Assessor's records also reveal that, in addition to the house, there is a garage and a shed located on the premises.

13. On or about June 10, 2011, I conducted a physical surveillance of 198 Concord Street, Portland, Maine. The residence is a multi-story building with white siding, black shutters, grey roof, and the numbers 198 above the stairs leading up to the front door. Adjacent to the residence is a white detached garage. I have attached a photograph that I took of that residence on June 10, 2011; it is marked as Exhibit 3.

14. At approximately 7:06 A.M. on or about June 14, 2011, I drove by 198 Concord Street, Portland, Maine, and observed a black Honda sport utility vehicle, bearing Maine license plate 5178LX, parked in the driveway. A review of Maine Bureau of Motor Vehicles (BMV) records revealed that vehicle is registered to Linda A. Fenton, born in 1950, registration address 198 Concord Street, Portland, Maine.

15. On June 23, 2011, a Federal Grand Jury Subpoena for account information for 198 Concord Street, Portland, Maine, was served upon Central Maine Power. Central Maine

Power's response revealed the billing name Linda A. Fenton for the service location 198 Concord Street, Portland, Maine. The records also revealed a premise phone of 207-774-0656 and customer name Linda A. Fenton, Social Security Number XXX-XX-1287, spouse John Fenton. The records include bill and payment history for 'Linda A. Fenton' from April 23, 2009 through June 22, 2011.

16. At approximately 7:37 P.M. on or about June 27, 2011, I conducted a physical surveillance at 198 Concord Street, Portland, Maine. I observed a Ford sport utility vehicle bearing Maine license plate 5541QA parked in the driveway. A review of Maine BMV records revealed that vehicle is registered to the organization Spurwink, registration address 899 Riverside Street, Portland, Maine. A review of public source information revealed that Spurwink Services is an "organization providing behavioral health, educational and residential services for children, adolescents, adults and families." Spurwink's internet web site listed John Fenton, LCSW, as the Associate Director of Clinical Services. At approximately 7:40 P.M. on that date, in the yard of 198 Portland Street, I observed a white male, bearing a resemblance to the Maine BMV photograph of John Fenton, born in 1949, whose photograph I received from the Maine BMV.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic

storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

19. As set forth above, probable cause exists to believe that an individual at 198 Concord Street in Portland, Maine has distributed, transported, received, or possessed child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

- a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification.

- b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.
- d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

20. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration

files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

21. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable, this includes as example but is not limited to extremely compact storage devices such as thumb-nail drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles.

22. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

- b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

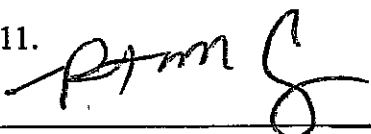
23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described

in the warrant, and then later review the seized items or image copies consistent with the warrant. *PMC 01/06/2011*
If any computers or electronic storage media are seized to enable further searching for contraband, the government shall report back to the court within fourteen (14) days.

CONCLUSION

24. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

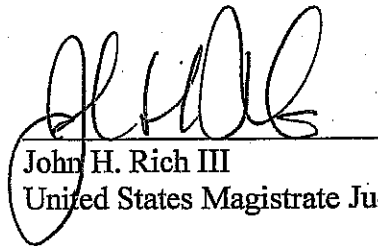
Dated at Portland, Maine this 6th day of July, 2011.


Patrick M. Clancy, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 6th day of July, 2011.

A TRUE COPY
ATTEST: Christa K. Berry, Clerk

By: 
Deputy Clerk


John H. Rich III
United States Magistrate Judge